# Cyber avenir de la police?

Autor(en): **Lüthi, Pascal**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2017)**

Heft 4

PDF erstellt am: **27.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-781589

Les villes et les autorités s'équipent et se digitalisent. Ci-contre, station de contrôle de la ville de Nice, en France.

*Police*

## Cyber avenir de la police ?

**Col Pascal Lüthi**
Commandant de la Police Neuchâteloise

Oubliez les flagrants délits ! L'efficacité de la police judiciaire a toujours progressé par révolutions à mesure des innovations scientifiques et technologiques liées à l'exploitation des traces matérielles. Ainsi, dès la fin du XIX[e] siècle, apparaissent les premiers fichiers d'empreintes digitales et les premières identifications de criminels basées sur leurs empreintes - marquant la fin du monopole millénaire des aveux et du témoignage dans la condamnation des auteurs. Et, contrairement aux arbitraires témoignages et aveux, les traces ne sauraient mentir. Mais leur prélèvement et leur analyse reposent sur des connaissances scientifiques et techniques spécifiques. La pertinence des preuves judiciaires gagnera ainsi en objectivité et deviendra désormais une question plus statistique que psychologique.

Les techniques de police scientifique n'ont depuis jamais cessé de s'améliorer, mais ce n'est qu'en 1985 qu'une nouvelle révolution va se mettre en route avec la découverte de l'ADN. Et pour la première fois en 1987, l'auteur d'un meurtre est identifié sur la base de son empreinte génétique (affaire Colin Pitchfork). Par la suite, la police va littéralement exploser son taux d'élucidation des affaires en affinant et en généralisant la méthode. Les révolutions de cet ordre sont rares, mais il ne fait aucun doute que la police se trouve aujourd'hui à l'aube d'une troisième (cyber)révolution avec la numérisation de la vie sociale, économique, politique et criminelle, et son cortège de nouvelles traces numériques exploitables.

Les spécialistes s'accordent à considérer qu'il y a globalement plus de matériel volé et « dealé » *par le biais d'Internet (au sens large) que par effractions, violences ou par vrais contacts physiques. Mais il faut d'emblée constater que la police n'y consacre encore qu'une part marginale de ses ressources et que cette nouvelle criminalité reste encore majoritairement cachée. Elle est toujours un tabou pour les personnes, un secret commercial pour les* entreprises, voire un secret d'Etat pour ceux qui en sont les victimes.

La prise de conscience est en marche depuis quelques années, mais ces nouvelles formes de criminalité restent moins anxiogènes, voire ignorées par une société et des politiques encore largement cybernaïves. Les gourous de la cybersécurité s'en inquiètent mais ils auraient tort de s'en offusquer car c'est le signe que cette menace n'a pas encore ébranlé la confiance générale et l'enthousiasme populaire dans toutes les nouvelles opportunités : e-commerce, e-banking, e-démocratie, etc.

Soyons clairs sur l'enjeu principal et l'objectif quand on aborde la question de la cybercriminalité. Le problème n'est pas l'existence de criminels dans le cyberespace et leur relative impunité. Il a toujours existé des malfrats capables de crocheter une porte ou de percer un coffre et n'oublions pas qu'il se commet en Suisse chaque jour plus de 100 cambriolages, dont 85 % ne seront jamais élucidés malgré l'excellent travail de la chaîne pénale. Ici, comme pour le reste de la criminalité, la mission n'est pas tant l'éradication d'un phénomène que le maintien d'un niveau acceptable de confiance permettant le développement pacifique des institutions, de l'économie et de la liberté individuelle.

Cependant, il est nécessaire et urgent aujourd'hui de rattraper un certain retard pris par la police et la justice cette dernière décennie sur la partie adverse, afin d'éviter une érosion rapide et préjudiciable de cette confiance.

Il s'agit premièrement d'une question inédite de compétence. Si tout le monde comprend aisément le fonctionnement d'une serrure ou d'une arme à feu, et le scénario d'un cambriolage ou d'un meurtre, l'ère numérique voit, pour la première fois dans l'histoire judiciaire, des délits que le simple bon sens est incapable d'appréhender - même sommairement. De plus, cette complexité rend

illusoire d'espérer que les utilisateurs puissent un jour adopter un comportement raisonnablement responsable face aux risques, à l'image de ce que nous faisons quand nous verrouillons nos portes, dissimulons nos valeurs ou gardons un secret. Enfin, ce mille-feuille technologique interconnecté interdit également d'imaginer ou d'exiger que l'industrie propose prochainement du matériel et des logiciels certifiés sûrs, sans failles et sans « bugs. » Mais la confiance dans les institutions exige que policiers et magistrats comblent rapidement leurs déficits de compétence et gagnent en crédibilité dans un domaine où seuls hackeurs et techniciens se disputent aujourd'hui l'autorité.

C'est pourquoi l'ensemble des polices de Suisse est désormais résolument engagé dans le développement coordonné des compétences nécessaires à la compréhension des phénomènes cybercriminels, la préservation et l'exploitation des traces numériques ainsi qu'à la conduite de cyberenquêtes dans les réseaux.

Ces connaissances doivent se décliner de façon pyramidale, en compétence de base pour l'ensemble des policiers de terrain, mais également en formation spécialisées pour enquêteurs ou inspecteurs scientifiques généralistes ou encore en développement d'expertises pointues en collaboration avec les hautes écoles et l'industrie.

Concrètement, la Conférence des Commandants des Polices Cantonales de Suisse (CCPCS) a lancé fin 2016, en collaboration avec l'Institut de Suisse de Police (ISP) et l'Institut de Lutte contre la Criminalité Economique (ILCE) de la Haute Ecole de Gestion (HEG) ARC à Neuchâtel, un projet d'*e-learning* destiné à combler le déficit de compétence de base de l'ensemble des policiers suisses d'ici à fin 2018. Les profils de compétences communs ainsi que des plans de formation pour les fonctions plus spécialisées sont également en développement sous l'égide de l'ISP.

Au-delà des questions de compétences, il s'agit deuxièmement d'une question inédite de souveraineté. La cybercriminalité se caractérise par une délocalisation et une dématérialisation complète des auteurs, des modus, des traces et même du butin alors que de son côté, la poursuite pénale fonctionne toujours sur l'articulation de souverainetés territoriales déclinées en fors juridiques et en processus d'entraide judiciaire.

A l'échelle suisse, il est désormais évident que ni la Confédération, ni aucun Canton - aussi grand soit-il - ne peut, à lui seul, se donner les moyens d'une poursuite pénale efficiente en matière de cybercriminalité sur son territoire. L'avenir passera par la création de quelques centres de compétences d'importance nationale impliquant Cantons et Confédération ainsi que la mise en place de processus de coordination et de priorisation des enquêtes allant bien au-delà de l'actuel Service de Coordination de la lutte contre la Criminalité sur Internet (SCOCI) - un défi, mais surtout une chance de redéfinir en profondeur le fédéralisme en matière de sécurité intérieure.


Mais comme l'ont montré certains récents succès (comme l'affaire DD4BC, Zurich), une enquête pénale contre des cybercriminels agissant de l'étranger selon des modus complexes, traversant des juridictions multiples, nécessite aujourd'hui des ressources souvent sans commune mesure avec les dommages causés. Ce n'est pas tant l'inadéquation des lois qui limite l'action, mais bien plus l'asymétrie entre des délits automatisés rapides et bon marché d'un côté et des enquêtes manuelles lentes et chères de l'autre.

Au point qu'on peut se demander si l'application du droit tel qu'on le connaît est le bon paradigme pour atteindre l'objectif sécuritaire souhaité dans cet espace sans frontières. Peut-être devrait-on développer, en collaboration avec les fournisseurs de services, des approches alternatives basées sur une détection automatisée des phénomènes (à l'image de nos radars sur les routes) et viser des objectifs plus sécuritaires que judiciaires. C'est-à-dire prioriser l'arrêt de l'agression, la destruction des connexions, quand c'est possible, sans forcément toujours viser la condamnation improbable d'un auteur.

P. L.